

1 COOLEY LLP  
2 MICHAEL G. RHODES (116127)  
(rhodesmg@cooley.com)  
3 KYLE C. WONG (224021)  
(kwong@cooley.com)  
4 AARTI G. REDDY (274889)  
(areddy@cooley.com)  
5 101 California Street, 5th Floor  
6 San Francisco, CA 94111-5800  
Telephone: (415) 693-2000  
Facsimile: (415) 693-2222

7 CHARLES A. WOOD (310702)  
(cwood@cooley.com)  
8 1299 Pennsylvania Ave., NW, Suite 700  
Washington, DC 20004  
9 Telephone: (202) 842-7800  
Facsimile: (202) 842-7899

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

17 AUDRA GRAHAM and STACY MOISE,  
18 individually and on behalf of all others  
similarly situated,

19 | Plaintiffs.

20 || v.

21 || NOOM, INC. and FULLSTORY, INC.

22 || Defendants.

Case No. 3:20-cv-06903-LB

**DEFENDANT NOOM, INC.'S MOTION TO  
DISMISS PLAINTIFFS' SECOND AMENDED  
CLASS ACTION COMPLAINT PURSUANT TO  
FEDERAL RULES OF CIVIL PROCEDURE  
12(B)(1) AND 12(B)(6)**

Hearing Date: July 29, 2021  
Hearing Time: 9:30 a.m.  
Judge: Honorable Laurel Beeler

## **NOTICE OF MOTION AND MOTION TO DISMISS**

2 PLEASE TAKE NOTICE that on July 29, 2021, at 9:30 a.m., or as soon thereafter as the  
3 motion may be heard in Courtroom B, 15th Floor of the San Francisco Courthouse, located at 450  
4 Golden Gate Avenue, San Francisco, CA 94102, pursuant to Federal Rules of Civil Procedure  
5 12(b)(1) and 12(b)(6), defendant Noom, Inc. (“Noom”) will and hereby does move to dismiss the  
6 causes of action in plaintiffs Audra Graham and Stacy Moise’s (“Plaintiffs”) Second Amended  
7 Class Action Complaint filed on April 29, 2020 (ECF No. 58) (“SAC”). This motion is based on  
8 this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the  
9 declaration of Aarti G. Reddy, the Request for Judicial Notice and Incorporation by Reference, the  
10 pleadings on file in this matter, oral argument of counsel, and such other materials and argument  
11 as may be presented in connection with the hearing of the motion.

## STATEMENT OF RELIEF SOUGHT

13 Noom respectfully seeks an order dismissing the SAC's causes of action with prejudice for  
14 lack of standing and failure to state a claim upon which relief can be granted.

## **STATEMENT OF ISSUES TO BE DECIDED**

16       1.     Whether Plaintiffs state a claim under the California Invasion of Privacy Act  
17     ("CIPA"), California Penal Code Sections 631 and 635.

18           2.     Whether Plaintiffs have Article III standing to pursue a claim under Section 635 of  
19     CIPA.

20           3.    Whether Plaintiffs state a claim under the California Constitution for Invasion of  
21           Privacy.

22           4.     Whether Plaintiffs have Article III standing to pursue their claims for injunctive  
23 relief.

24

25

26

27

28

1 TABLE OF CONTENTS  
2

	Page
I. INTRODUCTION .....	1
II. BACKGROUND. ....	2
III. LEGAL STANDARD.....	5
IV. THE SAC FAILS TO STATE A CLAIM. ....	6
A. Plaintiffs Fail to State a Claim Under CIPA. ....	6
1. Plaintiffs Fail to Allege the Elements of a Section 631 Violation. ....	6
a. Noom cannot be liable for “aiding” or “conspiring” to listen to its own communications. ....	7
b. Noom is also not liable for aiding and abetting because FullStory did not violate Section 631. ....	9
c. Even if FullStory’s technology is a wiretap, Plaintiffs fail to plead that the content of their communications was intercepted. ....	14
2. Plaintiffs Fail to Allege Sufficient Facts to Support a Section 635 Claim. ....	15
a. Plaintiffs lack constitutional or statutory standing to bring a Section 635 claim against Noom. ....	16
b. FullStory’s technology is not a device “primarily or exclusively designed” for eavesdropping.....	17
B. Plaintiffs Fail to Allege an Invasion of Privacy Under the California Constitution. ....	19
1. Plaintiffs Fail to Allege a Legally Protected Privacy Interest.....	20
2. Plaintiffs Fail to Allege a Reasonable Expectation of Privacy. ....	21
3. Plaintiffs Fail to Allege Noom’s Conduct Was a Serious Invasion of Privacy. ....	23
V. PLAINTIFF MOISE’S CLAIMS FOR INJUNCTIVE RELIEF SHOULD BE DISMISSED PURSUANT TO RULE 12(B)(1) BECAUSE SHE LACKS STANDING. ....	25
VI. CONCLUSION.....	25

1 TABLE OF AUTHORITIES  
2

	Page(s)
3 <b>Cases</b>	
4 <i>Alch v. Superior Ct.</i> , 5         165 Cal. App. 4th 1412 (2008) .....	21
6 <i>Allen v. Quicken Loans Inc.</i> , 7         No. 17-12352, 2018 WL 5874088 (D.N.J. Nov. 9, 2018) .....	15
8 <i>Associated Gen. Contractors v. Metro. Water Dist.</i> , 9         159 F.3d 1178 (9th Cir. 1998).....	5
10 <i>Belluomini v. Citigroup, Inc.</i> , 11         No. CV 13-01743, 2013 WL 3855589 (N.D. Cal. July 24, 2013) .....	19
12 <i>Brodsky v. Apple Inc.</i> , 13         445 F. Supp. 3d 110 (N.D. Cal. 2020) .....	9
14 <i>Cabral v. Supple, LLC</i> , 15         No. EDCV 12-85, 2012 WL 12895825 (C.D. Cal. Oct. 3, 2012).....	20
16 <i>Cahen v. Toyota Motor Corp.</i> , 17         717 F. App'x 720 (9th Cir. 2017) .....	17
18 <i>City of Los Angeles v. Lyons</i> , 19         461 U.S. 95 (1983).....	25
20 <i>Cohen v. Casper Sleep, Inc.</i> , 21         Nos. 17cv9325, 17cv9389, 17cv9391, 2018 WL 3392877 (S.D.N.Y. July 12, 22         2018) .....	16, 22
23 <i>Contra Smith v. Fresno Irrigation Dist.</i> , 24         72 Cal. App. 4th 147 (1999) .....	20
25 <i>Davidson v. Kimberly-Clark Corp.</i> , 26         889 F.3d 956 (9th Cir. 2018).....	25
27 <i>DirecTV, Inc. v. Treworgy</i> , 28         373 F.3d 1124 (11th Cir. 2004).....	17
29 <i>In re DoubleClick, Inc. Priv. Litig.</i> , 30         154 F. Supp. 2d 497 (S.D.N.Y. 2001).....	18
31 <i>Dyloco v. Mazda Motor of Am., Inc.</i> , 32         No. 3:20-cv-09099 (N.D. Cal. Apr. 13, 2021), ECF No. 36.....	2
33 <i>Eminence Cap., LLC v. Aspeon, Inc.</i> , 34         316 F.3d 1048 (9th Cir. 2003).....	25

## TABLE OF AUTHORITIES (continued)

Page(s)	
2	<i>In re Facebook Internet Tracking Litig.</i> , 263 F. Supp. 3d 836 (N.D. Cal. 2017) ..... 18
4	<i>In re Facebook, Inc. Internet Tracking Litig. (Facebook)</i> , 956 F.3d 589 (2020)..... <i>passim</i>
6	<i>Folgelstrom v. Lamps Plus, Inc.</i> , 195 Cal. App. 4th 986 (2011) ..... 23
7	<i>Friends of Yosemite Valley v. Norton</i> , 348 F.3d 789 (9th Cir. 2003)..... 18
9	<i>In re Google Android Consumer Priv. Litig.</i> , No. 11-MD-02264, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013)..... 24
11	<i>In re Google Inc. Cookie Placement Consumer Priv. Litig.</i> , 806 F.3d 125 (3d Cir. 2015)..... 7
12	<i>In re Google Location Hist. Litig.</i> , 428 F. Supp. 3d 185 (N.D. Cal. 2019) ..... 20, 21
14	<i>In re Google, Inc. Priv. Pol'y Litig.</i> , 58 F. Supp. 3d 968 (N.D. Cal. 2014) ..... 18, 23
15	<i>Hernandez v. Hillsides, Inc.</i> , 47 Cal. 4th 272 (2009) ..... 19
17	<i>Hill v. Nat'l Collegiate Athletic Ass'n</i> , 7 Cal. 4th 1 (1994) ..... 20, 21, 22
19	<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012) ..... 24
21	<i>Kendall v. Visa U.S.A., Inc.</i> , 518 F.3d 1042 (9th Cir. 2008)..... 6
22	<i>Kirch v. Embarq Mgmt. Co.</i> , 702 F.3d 1245 (10th Cir. 2012)..... 9
24	<i>In re Lenovo Adware Litig.</i> , No. 15-md-02624, 2016 WL 6277245 (N.D. Cal. Oct. 27, 2016) ..... 17
25	<i>London v. New Albertson's, Inc.</i> , No. 08-CV-1173, 2008 WL 4492642 (S.D. Cal. Sept. 30, 2008) ..... 21
27	<i>Low v. LinkedIn Corp.</i> , 900 F. Supp. 2d 1010 (N.D. Cal. 2012) ..... 18, 23

## TABLE OF AUTHORITIES (continued)

Page(s)	
2	<i>Luis v. Zang</i> , 833 F.3d 619 (6th Cir. 2016) (Batchelder, J. dissenting)..... 15
4	<i>Lujan v. Defs. of Wildlife</i> , 504 U.S. 555 (1992)..... 6
6	<i>Membrila v. Receivables Performance Mgmt., LLC</i> , No. 09-cv-2790, 2010 WL 1407274 (S.D. Cal. Apr. 6, 2010)..... 7
8	<i>Moreno v. S.F. Bay Area Rapid Transit Dist.</i> , No. 17-cv-02911, 2017 WL 6387764 (N.D. Cal. Dec. 14, 2017)..... 19
10	<i>NovelPoster v. Javitch Canfield Grp.</i> , 140 F. Supp. 3d 938 (N.D. Cal. 2014) ..... 16
12	<i>Onn v. Carnival Corp.</i> , No. 5:20-cv-07929 (N.D. Cal. Apr. 12, 2021), ECF No. 65..... 2
14	<i>Padilla v. Yoo</i> , 678 F.3d 748 (9th Cir. 2012)..... 5
16	<i>In re Palmdale Hills Prop., LLC</i> , 654 F.3d 868 (9th Cir. 2011)..... 6
18	<i>Pareto v. FDIC</i> , 139 F.3d 696 (9th Cir. 1998)..... 6
20	<i>People v. Avery</i> , 27 Cal. 4th 49 (2002) ..... 6
22	<i>Powell v. Union Pac. R.R. Co.</i> , 864 F. Supp. 2d 949 (E.D. Cal. 2012)..... 7, 8, 9
24	<i>Raham v. Pac. Gas &amp; Elec. Co.</i> , No. 3:20-cv-09315 (N.D. Cal. April. 12, 2021), ECF No. 51..... 2
26	<i>Republic of Ecuador v. Mackay</i> , 742 F.3d 860 (9th Cir. 2014)..... 15
28	<i>Revitch v. New Moosejaw, LLC</i> , No. 18-cv-06827, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) ..... <i>passim</i>
2	<i>Revitch v. New Moosejaw, LLC</i> , No. 3:18-cv-06287 (N.D. Cal. May 1, 2019), ECF No. 40..... 15
4	<i>Revitch v. New Moosejaw, LLC</i> , No. 3:18-cv-06827 (N.D. Cal. May 22, 2019), ECF No. 43..... 14

## TABLE OF AUTHORITIES (continued)

Page(s)	
2	<i>Ribas v. Clark</i> , 38 Cal. 3d 355 (1985) ..... 8
3	
4	<i>Rogers v. Ulrich</i> , 52 Cal.App.3d 894, 125 Cal.Rptr. 306 (1975) ..... 3, 7, 8, 10
5	
6	<i>Ruiz v. Gap, Inc.</i> , 540 F. Supp. 2d 1121 (N.D. Cal. 2008), <i>aff'd</i> , 380 F. App'x 689 (9th Cir. 2010) ..... 24
7	
8	
9	<i>Saleh v. Nike, Inc.</i> , No. 2:20-cv-09581 (C.D. Cal. Dec. 14, 2020), ECF No. 19 ..... 5
10	
11	<i>Scott v. Breeland</i> , 792 F.2d 925 (9th Cir. 1986) ..... 6
12	
13	<i>In re Sony Grand Wega KDF-E A10/A20 Series Rear Projection HDTV Television Litig.</i> , 758 F. Supp. 2d 1077 (S.D. Cal. 2010) ..... 11
14	
15	<i>Spokeo, Inc. v. Robins</i> , 136 S. Ct. 1540 (2016) ..... 16
16	
17	<i>In re Vizio, Inc., Consumer Priv. Litig.</i> , 238 F. Supp. 3d 1204 (C.D. Cal. 2017) ..... 21
18	
19	<i>Warden v. Kahn</i> , 99 Cal. App. 3d 805 (1979) ..... 6
20	
21	<i>Watson v. Weeks</i> , 436 F.3d 1152 (9th Cir. 2006) ..... 6
22	
23	<i>White v. Lee</i> , 227 F.3d 1214 (9th Cir. 2000) ..... 6
24	
25	<i>In re Yahoo Mail Litig. (Yahoo)</i> , 7 F. Supp. 3d 1016 (N.D. Cal. 2014) ..... 19, 20, 22, 23
26	
27	<i>Yunker v. Pandora Media, Inc.</i> , No. 11-CV-03113, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) ..... 24
28	
29	<i>In re Zynga Priv. Litig.</i> , 750 F.3d 1098 (9th Cir. 2014) ..... 15

## TABLE OF AUTHORITIES (continued)

2		(continued)	
3	<b>Statutes</b>		
4	California Invasion of Privacy Act, Cal. Penal Code		
5	§ 631.....	<i>passim</i>	
6	§ 635.....	<i>passim</i>	
7	§ 637.2(a) .....	16	
8	Federal Wiretap Act, 18 U.S.C. § 2511, et. seq.	<i>passim</i>	
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			

1     **I. INTRODUCTION.**

2                   As this Court previously observed, Noom’s implementation of FullStory’s session replay  
 3 technology is not a wiretap. Rather, FullStory provides “software as a service” that collects website  
 4 information for Noom, as directed by Noom, and that Noom itself could collect. After three  
 5 attempts to plead a viable complaint, Plaintiffs still do not allege that FullStory independently  
 6 analyzes the data it collects for Noom, or that it disseminates, sells or uses that data for any of its  
 7 own purposes. Plaintiffs’ claims must once again be dismissed. Further, because any additional  
 8 amendment would be futile, the Court should now dismiss with prejudice.

9                   Plaintiffs’ core theory is that Noom should be held liable as an aider and abettor of  
 10 FullStory’s alleged wiretapping under Section 631 of CIPA. But that claim fails as each Plaintiff  
 11 voluntarily communicated with Noom’s website, and courts have long recognized that parties can  
 12 neither wiretap nor aid and abet a wiretap of their own communications. Even if Plaintiffs’ aiding  
 13 and abetting theory were otherwise viable, Plaintiffs’ claims would still fail as they have not pled  
 14 that FullStory is a third-party eavesdropper. The Ninth Circuit has held that courts must examine  
 15 the “technical context” of a case in applying the party exception to Section 631. Here, Plaintiffs  
 16 concede that “FullStory’s software [is] employed by Noom” as a “software-as-a-service (‘SaaS’)  
 17 company” (SAC ¶¶ 40, 12), and describe the many ways *Noom* (not FullStory) might be able to use  
 18 the data FullStory collects on Noom’s behalf. Plaintiffs’ contrived allegations that FullStory does  
 19 more with the data it collects are unconvincing. The SAC offers only stray quotes from patents and  
 20 a form agreement that are both untethered to Noom’s actual implementation of FullStory’s tools  
 21 and consistent with the conclusion that FullStory’s role is to collect and analyze website visitor data  
 22 for Noom, as specifically directed by Noom.

23                   Plaintiffs’ Section 635 claims also fail for myriad reasons. Not only have Plaintiffs failed  
 24 to plead an unlawful wiretap, they invite the Court to recognize a private right of action under  
 25 Section 635 in contravention of the clear statutory language of Section 637.2, fail to allege how  
 26 Noom’s possession of FullStory’s code caused them any injury, and do not properly plead—as they  
 27 must—that FullStory’s code is a device “primarily or exclusively designed or intended for  
 28 eavesdropping.”

1 Plaintiffs also fail to sufficiently plead an invasion of privacy that meets the high bar for  
 2 violations of the California Constitution. As Plaintiffs cannot even recall what information they  
 3 provided on the Noom website, they cannot demonstrate a reasonable expectation of privacy  
 4 regarding information they freely provided to a public website that was never disseminated beyond  
 5 that website's service provider. (*Id.* ¶¶ 4, 5.)

6 Plaintiffs' inability to state a claim for relief is unsurprising; the conduct that Plaintiffs seek  
 7 to criminalize encompasses an extraordinary volume of routine communications that take place  
 8 many times every second for almost every website on the Internet. Were this Court to allow such  
 9 claims to proceed, countless service providers that collect and analyze data on behalf of websites—  
 10 ranging from Amazon Web Services to Google Analytics—could be subject to severe penalties, as  
 11 would the websites that hire them. The Court should decline Plaintiffs' invitation to drastically  
 12 expand the scope of California wiretapping and privacy laws, opening the litigation floodgates.

13 Since Noom's last motion to dismiss, Plaintiffs' counsel have voluntarily dismissed several  
 14 of the many copycat session replay cases they had filed in this District.<sup>1</sup> With good reason, as  
 15 service providers like FullStory are not wiretaps. This Court should once again dismiss Plaintiffs'  
 16 claims, this time with prejudice.

17 **II. BACKGROUND.**

18 Defendant Noom operates a mobile application that helps millions of users lose weight and  
 19 lead healthier lives. (SAC ¶¶ 62, 7.) Plaintiffs Audra Graham and Stacy Moise each claim to have  
 20 visited the Noom website and input unspecified information. (*Id.* ¶¶ 4, 5.) According to Plaintiffs,  
 21 during these visits, Noom “recorded” their “keystrokes, mouse clicks, and other electronic  
 22 communications” using tools provided by its “software-as-a-service” provider, Defendant  
 23 FullStory, Inc. (*Id.* ¶¶ 1, 72, 12.) Plaintiffs further contend that this “recording” was an unlawful  
 24 wiretap that violated Cal. Penal Code §§ 631 and 635 and the California Constitution. (*Id.* ¶ 1.)

25 Noom and FullStory previously moved to dismiss Plaintiffs' First Amended Complaint.

---

26 <sup>1</sup> Notice of Voluntary Dismissal without Prejudice, *Dyloco v. Mazda Motor of Am., Inc.*, No.  
 27 3:20-cv-09099 (N.D. Cal. Apr. 13, 2021), ECF No. 36; Notice of Voluntary Dismissal without  
 28 Prejudice, *Onn v. Carnival Corp.*, No. 5:20-cv-07929 (N.D. Cal. Apr. 12, 2021), ECF No. 65;  
 Notice of Voluntary Dismissal without Prejudice, *Raham v. Pac. Gas & Elec. Co.*, No. 3:20-cv-  
 09315 (N.D. Cal. April. 12, 2021), ECF No. 51.

1 The Defendants argued, *inter alia*, that: (1) Noom could not wiretap or aid and abet wiretapping  
 2 because it is a party to the allegedly intercepted communications, (*see* ECF No. 36 at 7-8); and (2)  
 3 FullStory’s recording of Noom’s communications was not an unlawful wiretap because FullStory  
 4 is only a service provider that stands in the shoes of Noom and collects data on Noom’s behalf.  
 5 (ECF No. 35 at 10-13.)<sup>2</sup> The Court dismissed the First Amended Complaint on the latter grounds.  
 6 (ECF No. 51 at 2.) In particular, the Court held that FullStory “provides a tool—like the tape  
 7 recorder in *Rogers*—that allows Noom to record and analyze its own data in aid of Noom’s  
 8 business. It is not a third-party eavesdropper. As a result, Noom is not liable for aiding and abetting  
 9 FullStory’s wrongdoing because there is no wrongdoing.” (*Id.* at 9.) Moreover, at the dismissal  
 10 hearing, the Court highlighted that FullStory provides “a platform for analytics” and questioned  
 11 how the provision of such a platform was sufficient to establish “liability for third-party  
 12 eavesdropping.” (ECF No. 56 at 11.) At that same hearing, Plaintiffs’ counsel tacitly admitted that  
 13 FullStory acts as Noom’s service provider, stating that “FullStory does just provide it to Noom”  
 14 and suggested that there would be no wiretap “if Noom or Blue Nile had some proprietary session  
 15 replay software and they were to do the recording themselves on their own website.” (*Id.* at 10:21;  
 16 9:6-8.)

17 On April 29, 2021, Plaintiffs filed a Second Amended Complaint in which they continue to  
 18 allege that FullStory is a “software-as-a-service” provider and focus on FullStory’s general role in  
 19 facilitating access to data analytics for unspecified website providers. (*E.g.*, SAC ¶ 26 (“FullStory  
 20 *lets a company* view the video of a user’s interaction with a website”) (*emphasis added*); *id.* at 32  
 21 (“FullStory . . . *allows websites* to monitor [users] *live*”) (*emphasis added*)).

22 Plaintiffs’ core allegations have not changed. The SAC asserts the same causes of action  
 23 and the same theory of liability that this Court previously dismissed—i.e., “FullStory’s software,  
 24 as employed by Noom, functions as a wiretap.” (SAC ¶ 40.) Plaintiffs do not describe in detail  
 25 how FullStory’s technology is purportedly implemented by Noom. Instead, they include alleged  
 26 screen shots of *a* FullStory tool operating on *a* hypothetical website but offer no detailed allegations

27  
 28 <sup>2</sup> Plaintiffs filed their original complaint on October 2, 2020. (ECF No. 1.) Noom and FullStory  
 filed motions to dismiss raising many of the same arguments presented here. (ECF Nos. 25, 26.)  
 Rather than opposing these motions, Plaintiffs amended their complaint. (ECF No. 27.)

1 describing how *Noom* implemented a specific FullStory technology, which FullStory then used to  
 2 collect and transmit Plaintiffs' information to itself.<sup>3</sup> (*Id.* ¶¶ 20-28.) Plaintiffs also allege again  
 3 that "Noom knows that FullStory's software captures the keystrokes, mouse clicks and other  
 4 communications of visitors," that it "pays FullStory to supply that information" and that "upon  
 5 information and belief, the Session Replay feature in FullStory's software captured each of  
 6 Plaintiffs' keystrokes, mouse clicks, and other electronic communications on the website, which it  
 7 then analyzed and compiled into a recording."<sup>4</sup> (*Id.* ¶¶ 38, 53.) The SAC, however, does not  
 8 describe any keystroke, mouse click, or other communications that FullStory and Noom allegedly  
 9 captured. Similarly, while Plaintiffs claim to have input "at least some . . . personal or medical  
 10 information" on Noom's website, they do not detail the information they disclosed to Noom or  
 11 describe how they were harmed by Noom's and FullStory's collection of that data. (*Id.* ¶¶ 4, 5.)

12 Plaintiffs also attempt to demonstrate that FullStory is more than just a service provider to  
 13 Noom by adding several new allegations regarding FullStory's hypothetical ability to analyze data  
 14 on unspecified websites. First, the SAC offers stray quotes from two alleged FullStory patents.  
 15 (*Id.* ¶¶ 41-46.) But the SAC notably fails to allege that these patents are related to the software at  
 16 issue in this case—i.e., FullStory's session replay technology as implemented on Noom's website.  
 17 Indeed, the SAC does not allege that the technology described in these patents was ever even  
 18 incorporated into *any* of FullStory's technology. The features discussed in these patents, moreover,  
 19 are all those that a service provider might offer, such as: transmitting and storing data generated

20 \_\_\_\_\_  
 21 <sup>3</sup> Plaintiffs reuse an online article purporting to provide a general description of "[s]ession replay  
 22 technology" that is not specific to either FullStory or Noom. (SAC ¶ 20 n.4.) The article goes on  
 23 to admit that "there is no known case of a compromise of user data due to session replay scripts."  
 24 (*Id.*) Plaintiffs also cite an article that undermines their own allegations by stating that "[m]ost  
 25 session replay tools don't rely on actual video . . . [r]ather, they reconstruct events as they  
 26 occurred." (*Id.* ¶ 21 n.5). Likewise, Plaintiffs again repeatedly reference a 2017 blog post they  
 27 optimistically call a "study by Princeton University," that is neither cited nor attached to their SAC.  
 28 (*Id.* ¶¶ 29, 33, 34, 69.) This blogpost purports to comment on FullStory's functionality on a  
 different website (Walgreen's) and is in no way linked to Noom.

<sup>4</sup> Plaintiffs incorrectly allege that Noom's Privacy Policy fails to account for services such as  
 FullStory's. (*Id.* ¶ 67 (claiming that Noom's disclosure that it "may" collect such information is  
 "vague.")) In fact, that policy states that "Noom may use various methods and technologies to  
 store or collect Usage information" including by employing "programming code that is designed  
 to collect information about User's interactions with the Website. . . . such as the links User clicks  
 on." *Privacy Policy*, Noom (Dec. 17, 2018), <https://web.noom.com/terms-and-conditions-of-use/noom-privacy-policy/>. As used here "May" indicates that FullStory's code collects *some* but  
 not *all* visitors' information—a common feature of session replay tools.

1 by a website visitor (*id.* at ¶ 41); indexing that same information to allow website owners to search  
 2 for specific events (e.g., a point where the website malfunctions) (*id.* at ¶ 43); identifying contextual  
 3 clues within data from a website visit (e.g., whether clicking a link led to a site error) (*id.* at ¶ 44);  
 4 and allowing pairing of data from the website publisher's own databases (*id.* ¶ 46). Furthermore,  
 5 each of these alleged features is couched in provisional language such as "can be transmitted" (*id.*  
 6 at ¶ 42), "[i]n some implementations" (*id.* at ¶¶ 43, 46), and "can analyze" (*id.* at ¶ 44)—leaving it  
 7 unclear what features Plaintiffs allege FullStory provided to Noom.

8 Second, Plaintiffs point to FullStory's Partner Terms and Conditions as supposed evidence  
 9 that FullStory "has access to the communications recorded by its software." (*Id.* ¶ 48.) Setting  
 10 aside the fact that service providers often access data to provide a service, Plaintiffs do not claim  
 11 that Noom's agreement with FullStory contains the "standard Partner Terms and Conditions," nor  
 12 do they contend that FullStory actually accessed or used any of the communications it allegedly  
 13 recorded on Noom's behalf. (*Id.*)

14 Finally, Plaintiffs amass various citations to instances where FullStory has argued in legal  
 15 filings that it should be treated as "a party" to communications captured by its technology,  
 16 insomuch as it steps into the shoes of its customers as a service provider (*Id.* ¶¶ 56, 57). *See, e.g.*,  
 17 Defs. Notice of Mot. and Mot. to Dismiss at 2:14-17, *Saleh v. Nike, Inc.*, No. 2:20-cv-09581 (C.D.  
 18 Cal. Dec. 14, 2020), ECF No. 19 ("Nike and FullStory fit within the well-recognized party  
 19 exception under CIPA. Because FullStory was not a third party to the communication, but instead  
 20 an extension of Nike, neither Nike nor FullStory can be held liable for eavesdropping under Section  
 21 631."). However, this legal argument does not, as Plaintiffs contend, amount to an "admi[ssion]  
 22 that [FullStory] accessed communications" other than as a service provider. (SAC ¶ 56).

23 **III. LEGAL STANDARD.**

24 Rule 12(b)(6) provides for dismissal of an action for "failure to state a claim upon which  
 25 relief can be granted." *See* Fed. R. Civ. P. 12(b)(6). For a 12(b)(6) motion, "all well-pleaded  
 26 allegations of material fact [are accepted as true] and construe[d] in the light most favorable to the  
 27 non-moving party." *Padilla v. Yoo*, 678 F.3d 748, 757 (9th Cir. 2012). "[C]onclusory allegations  
 28 of law and unwarranted inferences" are insufficient. *Associated Gen. Contractors v. Metro. Water*

1 *Dist.*, 159 F.3d 1178, 1181 (9th Cir. 1998) (citing *Pareto v. FDIC*, 139 F.3d 696, 699 (9th Cir. 2  
2 1998)). A complaint must state “evidentiary facts which, if true, will prove [the claim],” *Kendall*  
3 *v. Visa U.S.A., Inc.*, 518 F.3d 1042, 1047 (9th Cir. 2008), otherwise it will be dismissed. *See Watson*  
4 *v. Weeks*, 436 F.3d 1152, 1157 (9th Cir. 2006).

5 A challenge to a federal court’s subject matter jurisdiction is properly raised under a motion  
6 to dismiss pursuant to Rule 12(b)(1). *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). “Article  
7 III standing is a necessary component of subject matter jurisdiction.” *In re Palmdale Hills Prop.,*  
8 *LLC*, 654 F.3d 868, 873 (9th Cir. 2011). Standing requires that the plaintiff suffered an “injury in  
9 fact” that is “concrete and particularized.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). In  
10 seeking to invoke a court’s jurisdiction, plaintiffs bear the burden of proving that jurisdiction exists.  
11 *Scott v. Breeland*, 792 F.2d 925, 927 (9th Cir. 1986).

12 **IV. THE SAC FAILS TO STATE A CLAIM.**

13 **A. Plaintiffs Fail to State a Claim Under CIPA.**

14 As set forth below, Plaintiffs fail to state a claim under either Sections 631 or 635 of CIPA  
15 and do not have standing under Section 635. Notably, to the extent there is any ambiguity in the  
16 application of CIPA to either FullStory or Noom, that ambiguity should be construed in  
17 Defendants’ favor. *People v. Avery*, 27 Cal. 4th 49, 58 (2002) (“ambiguous penal statutes are  
18 construed in favor of defendants . . . [if] two reasonable interpretations of the same provision stand  
19 in relative equipoise.”); *see Warden v. Kahn*, 99 Cal. App. 3d 805, 814, 818 n.3 (1979) (observing  
20 that as a penal statute, ambiguity in Section 631 should be interpreted narrowly).

21 **1. Plaintiffs Fail to Allege the Elements of a Section 631 Violation.**

22 Plaintiffs allege that Noom “purposefully aided and abetted FullStory’s” wiretap of Noom’s  
23 website in contravention of Section 631. (*Id.* ¶¶ 16, 66, 72.) To state a claim under the statute,  
24 Plaintiffs must plead facts showing that FullStory used a “machine, instrument, or contrivance” to  
25 make an “unauthorized connection with any telegraph or telephone wire, line, cable, or instrument,”  
26 that Noom aided and abetted this unlawful conduct, and that Noom is not exempt from such liability  
27 as a party to the communications. (*Id.* ¶ 83.) *See also* Cal. Penal Code § 631(a). The SAC fails to  
28 plead these elements.

- a. Noom cannot be liable for “aiding” or “conspiring” to listen to its own communications.

Noom cannot be held liable under a Section 631 aiding and abetting theory of liability because it was indisputably a party to the communication with Plaintiffs. (SAC ¶ 39, “FullStory . . . surreptitiously collect[ed] interactions between Noom and website users.”) *See Powell v. Union Pac. R.R. Co.*, 864 F. Supp. 2d 949, 954-55 (E.D. Cal. 2012) (granting a motion for summary judgment as to Section 631 aiding and abetting claims against a first party “[g]iven the settled nature of the third-party focus of section 631”).

As this Court previously recognized, “[o]nly a third party can listen to a conversation secretly. . . . By contrast, a party to a communication can record it (and it is not eavesdropping when it does).” ECF No. 51 at 7 (citation omitted). This observation is consistent with well-settled authority holding that Section 631 applies “only to eavesdropping by a third party.” *Membrila v. Receivables Performance Mgmt., LLC*, No. 09-cv-2790, 2010 WL 1407274, at \*2 (S.D. Cal. Apr. 6, 2010) (citation omitted); *see also In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 152 (3d Cir. 2015) (affirming the dismissal of Section 631 claims because “the pleadings demonstrate that Google was itself a party to all the electronic transmissions that are the bases of the plaintiffs’ wiretapping claims [] [b]ecause § 631 is aimed only at ‘eavesdropping, or the secret monitoring of conversations by third parties’”). As this Court noted in its dismissal of the FAC, in *Rogers v. Ulrich*, the court affirmed an order dismissing Section 631 claims when the defendant allegedly recorded his telephone conversation with the plaintiff. 52 Cal. App. 3d 894, 899 (1975). In so holding, the *Rogers* Court explained that “it is never a secret to one party to a conversation that the other party is listening to the conversation” and “‘Eavesdropping’ is the problem the Legislature meant to deal with” in enacting CIPA, which “is defined in Webster’s 7th New Collegiate Dictionary (1972) as ‘to listen secretly to what is said in private.’” *Id.*

The same logic that limits direct liability for parties under Section 631 also limits aiding and abetting liability. Section 631 is intended to prevent *third parties* that either wiretap or aid and abet wiretapping, not first parties who necessarily have access to the underlying communications. There is no other logical reading of Section 631 and Plaintiffs have cited no authority to the contrary.

1 other than *Revitch*, which is distinguishable as discussed below.

2 *Powell* is one of the only reported cases to directly address potential aiding and abetting  
 3 liability of a party to the communication—an indication of how clearly inapplicable Section 631 is  
 4 to aiding and abetting claims against parties. In that case, the plaintiff alleged that a union officer  
 5 eavesdropped on a phone call with his former union supervisor. He later asserted aiding and  
 6 abetting claims against his former supervisor, who was a party to the communication and permitted  
 7 the alleged eavesdropping. *Id.* at 954. The plaintiff in *Powell* “contend[ed] that the language of  
 8 section 631 is clear and a participant should be liable for aiding or conspiring with a third party to  
 9 enable that party to listen in on the call.” *Id.* Like *Noom*, the defendant argued that “section 631(a)  
 10 applies to third party actions and therefore, as a party to the call, he cannot be liable as a matter of  
 11 law.” *Id.* Carefully surveying longstanding precedent, the court agreed with defendant, stating:

12 Section 631 was aimed at one aspect of the privacy problem—  
 13 eavesdropping, or the secret monitoring of conversations by third  
 14 parties. . . . The third party focus of section 631 is confirmed by  
 15 *Rogers v. Ulrich*, 52 Cal.App.3d 894, 125 Cal.Rptr. 306 (1975),  
 16 where the court held that only a third party could violate the section  
 17 631 proscription on eavesdropping. . . . Given the settled nature of  
 18 the third-party focus of section 631, the court declines to adopt  
 19 plaintiff’s alternate reading.

20 *Id.* at 955-56 (internal quotation marks and citation omitted). In observing the “third-party focus”  
 21 of Section 631, the *Powell* court examined years of CIPA precedent. Further, *Powell* is consistent  
 22 with *Ribas* because the defendant there was a separate party—a third party eavesdropping on a  
 23 telephone line—and not an intended recipient of the communication between husband and wife.  
 24 *Id.* at 955 (citing *Ribas v. Clark*, 38 Cal. 3d 355, 359 (1985)).

25 *Rogers* also unequivocally affirms that Section 631 only criminalizes eavesdropping by  
 26 **third parties.** See *Rogers*, 52 Cal. App. 3d at 897-99. In *Rogers*, the defendant recorded his  
 27 conversation with plaintiff using “a tape recorder jack [that] had been recently installed on [his]  
 28 telephone by the telephone company.” 52 Cal. App. 3d at 897. The plaintiff there did not assert  
 the defendant aided and abetted wiretapping by the telephone company based on its provision of  
 tools to record the conversation. Like here, this would be absurd.

This interpretation of CIPA mirrors the federal Wiretap Act, which also exempts from

1 liability parties to the communication. 18 U.S.C. § 2511(2)(c), (d). “Courts perform the same  
 2 analysis for both the Wiretap Act and CIPA regarding the party exemption.” *In re Facebook, Inc.*  
 3 *Internet Tracking Litig. (Facebook)*, 956 F.3d 589, 607 (2020); *see also Brodsky v. Apple Inc.*, 445  
 4 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (“The analysis for a violation of CIPA is the same as that  
 5 under the federal Wiretap Act.”) (citation omitted). That statute also does not allow for *any* aiding  
 6 and abetting liability, and thus Plaintiffs’ attempt to impute a broad construction of aiding and  
 7 abetting liability under CIPA is fundamentally inconsistent with an identical analysis under both  
 8 statutes. *Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1247 (10th Cir. 2012) (stating that “[a]ny  
 9 temptation to read the statute as imposing aider-and-abettor liability is overcome by the  
 10 illuminating statutory history of the civil-liability provision[,]” and concluding that “almost all  
 11 courts to address the issue have held that § 2520 does not impose civil liability on aiders or  
 12 abettors”). Consistent with *Powell* (the only reasoned case on point) and the federal Wiretap Act,  
 13 Section 631 should not be drastically expanded to encompass parties to the communication.

14 Plaintiffs should find no solace in the recent *Revitch* decision, in which the Court misapplied  
 15 this case law and incorrectly denied dismissal of a claim against a first party to a purported  
 16 communication for “enabling” wrongdoing by a third party. *Revitch v. New Moosejaw, LLC*,  
 17 No. 18-cv-06827, 2019 WL 5485330, at \*2 (N.D. Cal. Oct. 23, 2019). Notably, the Court in  
 18 *Revitch*’s five-sentence analysis failed to articulate a reasoned basis for its contravention of  
 19 well-established precedent. Noom is not aware of any other case disputing the holding in *Powell*  
 20 that a party to a communication like Noom cannot be held liable for aiding and abetting under  
 21 CIPA, the federal Wiretap Act, or other state analogs. Accordingly, *Revitch* is an outlier and this  
 22 Court should decline to follow it. To decide otherwise would radically alter the scope of  
 23 California’s eavesdropping law, and inundate California courts with a deluge of litigation—not  
 24 unlike Plaintiffs’ counsel’s recent filing of over a dozen similar copycat lawsuits across California.

25 **b. Noom is also not liable for aiding and abetting because FullStory  
 26 did not violate Section 631.**

27 Even if Plaintiffs could circumvent the party exception to bring an aiding and abetting  
 28 claim, their claim would still fail because there was no statutory violation by FullStory to abet.

1           Rogers unequivocally affirms that Section 631 only criminalizes eavesdropping by *third*  
 2 *parties*. *See Rogers*, 52 Cal. App. 3d at 897-99. This Court previously recognized that “as a service  
 3 provider, FullStory is an extension of Noom,” and “the allegations about FullStory are different  
 4 than the acts that courts hold plausibly support a claim of surreptitious wiretapping by a third party.”  
 5 (ECF No. 51 at 7-8.) The thrust of Plaintiffs’ new allegations seek to create an inference that  
 6 FullStory is a non-party to any communications and is thus an unlawful third-party eavesdropper.  
 7 Plaintiffs incorrectly assert, for example, that FullStory’s actions were no different from the  
 8 situation CIPA was enacted to stop: “a person placing or receiving a call . . . where the person on  
 9 the other end of the line permits an outsider to tap his telephone or listen in on the call.” (SAC ¶  
 10 85, citations omitted). But Plaintiffs’ attempt at artful pleading does not save their claims.

11           The SAC still makes clear that FullStory is a vendor that provides a software as a service.  
 12 (SAC ¶ 12.) And nothing in Plaintiffs’ pleadings rebuts this Court’s finding that FullStory is  
 13 Noom’s vendor that “provides a software service that captures its clients’ data, hosts it on  
 14 FullStory’s servers, and allows [Noom] to analyze [its] data.” (See ECF No. 51 at 8); *supra* section  
 15 II. FullStory is not a data broker, like Navistone, nor is it an advertising platform, like Facebook.  
 16 The Defendants in those cases “were independent parties who mined information from other  
 17 websites and sold it” and Plaintiffs’ hodgepodge of new allegations regarding FullStory’s  
 18 technology do not compel a contrary conclusion. *Compare supra*, section II with ECF No. 51 at 8.

19           Given another chance to amend their complaint to allege that FullStory is more than just a  
 20 service provider, Plaintiffs have made only a few substantive additions: 1) allegations regarding  
 21 certain FullStory patent filings divorced from Noom and in accord with what features a service  
 22 provider might offer, 2) inapposite references to FullStory’s form partner development agreement,  
 23 and 3) a roundup of instances where FullStory has argued it is a party to communications it collects  
 24 on behalf of websites. *Supra* section II; (SAC ¶¶ 41-46; 4-5, 50-51; 89; 55-57.). None of these  
 25 new allegations create a plausible inference that FullStory’s role exceeds that of a service  
 26 provider—it collects and analyzes Noom’s data, as directed by Noom, and for Noom’s purposes.  
 27 And while Plaintiffs have omitted their prior allegation that FullStory’s purpose is to “help  
 28 businesses improve their website design and customer experience,” nothing in the SAC leads to a

1 different conclusion regarding FullStory’s limited role vis-à-vis Noom. (ECF No. 27 ¶ 18.)

2 **FullStory Patents.** Plaintiffs selectively quote two alleged FullStory patents that they do  
 3 not attach to their pleading, but Plaintiffs’ reliance on these documents is flawed for multiple  
 4 reasons. *First*, as a matter of law, any purported statements in the patent filings cannot show what  
 5 service FullStory provided because such filings speak generally to the state of the art (i.e., website  
 6 analytics technology), not a specific FullStory product. *See In re Sony Grand Wega KDF-E*  
 7 *A10/A20 Series Rear Projection HDTV Television Litig.*, 758 F. Supp. 2d 1077, 1090 (S.D. Cal.  
 8 2010) (giving no weight to patent filings, *inter alia*, because “Plaintiffs do not link any of the patent  
 9 filings to the” relevant product or service). Plaintiffs do not claim that any of the patents are used  
 10 in the session replay technology allegedly implemented by Noom, nor do they allege those patents  
 11 relate to that technology. Plaintiffs’ own pleading highlights the flaw in this omission,  
 12 acknowledging that session replay technology is just “[o]ne of FullStory’s features.” (SAC ¶ 18.)

13 *Second*, even assuming these patents were linked to the software actually deployed by  
 14 Noom, the inference Plaintiffs seek to draw regarding FullStory’s conduct are speculative at best.  
 15 Plaintiffs contend, for example, based on these patents, that FullStory “**can** combine its own session  
 16 replay information with other information obtained by website owners to provide a comprehensive  
 17 log of user activities,” “**can** analyze event data to identify specified events,” and “**can** obtain data  
 18 from other third-party applications.” (*Id.* ¶¶ 45, 44, 46 (emphases added).) Plaintiffs do not allege  
 19 that FullStory actually undertakes any of these hypothetical activities, let alone that it did so in  
 20 connection with its partnership with Noom or with Plaintiffs’ particular data.

21 *Third*, even if these cherry-picked quotes were linked to Noom’s use of FullStory, they  
 22 would be insufficient to allege that FullStory is more than Noom’s service provider. At most, these  
 23 allegations suggest that FullStory can index data so that it is more usable *by its website customers*,  
 24 associate attributes of a specific visit *so its website customers* can see all visits where X condition  
 25 occurs (such as a broken link), and append data its website customers provide to session replays  
 26 *for use by its website customers*, only. (*Id.* ¶¶ 41-46.) Yet all these activities (which are not  
 27 necessarily even utilized by Noom) are tools used as directed by the website operator, at the website  
 28 operator’s discretion—and thus fit squarely within a service provider’s role.

1       A careful review of each patent describes functionalities that underscore FullStory’s role as  
 2 a service provider of software that allows website operators to assess user interactions with their  
 3 website and identify and assess errors. To start, both patents claim to help websites assess “user  
 4 interaction with various resources and applications” and note that “[u]ser satisfaction with a given  
 5 website or application can depend on the user’s experience with the user interface,” generally refers  
 6 to the purpose of session replay software—i.e., a software provided as a service to assess user  
 7 interactions with a website. U.S. Patent No. 10,965,766, col. 1 l. 6-7 (filed June 13, 2019) (“Patent  
 8 1”); U.S. Patent No. 10,838,571, col. 1 l. 26-27 (filed Aug. 9, 2019) (“Patent 2”). Patent 1 describes  
 9 a tool that can create an animation from logs that would already be available to the website, and  
 10 goes on to explain that the technology it describes is meant to “enable[] the user interface  
 11 developers to more easily assess the effects of errors and to more easily diagnose why the errors  
 12 are occurring.” Patent 1, col. 3 l. 12-13. This simply shows that the referenced technology helps  
 13 businesses improve their website design and customer experience. Patent 2 contains similar  
 14 language. It describes a tool that provides website operators with “a list of user interactions with  
 15 the [website] and timestamps specifying when each of the user interactions occurred” that can be  
 16 reconstituted into a recreation of the website visitor’s experience. Patent 2, col. 2 l. 11-13. This  
 17 patent also describes triggers, “e.g., failed content loads or aborted user sessions,” that could cause  
 18 a session to be recreated for the website operator to review and fix the underlying error. *Id.* at col.  
 19 3 l. 51-52. These activities are all consistent with a service provider that enables websites to  
 20 monitor user interactions to improve the user experience.

21       Next, and contrary to Plaintiffs’ claims, nothing in these patents alleges that FullStory  
 22 deanonymizes website visitors, creates profiles about website visitors, or does anything other than  
 23 organizing Noom’s data. (SAC ¶¶ 45, 46.) Plaintiffs claim that “FullStory can obtain data from  
 24 other third-party applications and combine that data with its session replays,” but their only support  
 25 is a quote from one of the patents discussing websites like Noom uploading “information that *the*  
 26 *publisher has stored* in association with the user identified.”<sup>5</sup> (*Id.* ¶ 46 (emphasis added).) This is  
 27

28       

---

<sup>5</sup> Plaintiffs concede that the references to “publisher” in these patents refer to the website owner.  
 (SAC ¶ 45.)

1 a far cry from *FullStory* deanonymizing, scanning computers, or otherwise building user profiles.  
 2 What Noom may do with data it has collected about users from other sources is immaterial to  
 3 *FullStory*'s liability for wiretapping. Tellingly, Plaintiffs do not allege that *FullStory* ever  
 4 independently assembled or used this information for marketing or ad targeting purposes, or that  
 5 the information collected was ever sold or shared by *FullStory*.

6 In sum, for all the reasons set forth above, even assuming these patents were linked to  
 7 Noom's use of session replay software, the "technical context" they describe do not create a  
 8 plausible inference that *FullStory* acted as a third-party eavesdropper. *See Facebook*, 956 F.3d at  
 9 607 (holding that the "technical context" is paramount in determining whether a listener is  
 10 eavesdropping or a party exempt from CIPA liability). At bottom, these patents describe a service  
 11 provider's tools for website operators to improve site functionality.

12 ***Partner Terms and Conditions.*** Plaintiffs quote "Partner Terms and Conditions" as  
 13 supposed support for their allegation that "FullStory has access to the communications recorded by  
 14 its software." (SAC ¶ 48.) Once again, Plaintiffs do not link that agreement to this case by failing  
 15 to allege that Noom agreed to these terms with *FullStory*. In any event, even assuming *FullStory*  
 16 had access to the communications it collected on Noom's behalf, Plaintiffs never allege that  
 17 *FullStory* actually accessed, used, or disclosed those communications in any fashion. Moreover,  
 18 mere access to those underlying communications does not automatically transform *FullStory* into  
 19 a third party instead of a service provider that acts on Noom's behalf.

20 ***FullStory's Role as a Party to the Communication.*** Plaintiffs further claim *FullStory* is  
 21 necessarily a non-party to the communication because it has referred to itself as a "party" to  
 22 communications with its website customers in legal filings in copycat lawsuits filed by the same  
 23 Plaintiffs' counsel. (*Id.* ¶¶ 55-57.) This is simply a different way of stating that *FullStory* steps  
 24 into the shoes of the website provider (such as Noom), and therefore falls within the party  
 25 exception. These out-of-context quotes are hardly well-pled factual allegations that "FullStory  
 26 intercepted and used the data for itself," and Plaintiffs' reliance on them does not save their claims.

27 Finally, although the Courts in *Facebook* and *Revitch* sustained CIPA claims at the  
 28 dismissal stage, they did so based on starkly different facts, ones that only underscore Plaintiffs'

1 pleading deficiencies here. In *Facebook*, plaintiffs alleged that the defendant was compiling a  
 2 cradle-to-grave profile of logged out users' browsing history *for its own purpose* and without users'  
 3 consent. *Facebook*, 956 F.3d at 607. While in *Revitch*, NaviStone captured the data,  
 4 de-anonymized it, and matched it with other databases, thereby creating its own marketing  
 5 databases of identified website visitors. Second Am. Compl. at 2 (¶ 1), 4–17 (¶¶ 9–46), *Revitch v.*  
 6 *New Moosejaw, LLC*, No. 3:18-cv-06827, (N.D. Cal. May 22, 2019), ECF No. 43. As this Court  
 7 recognized in its order dismissing the FAC, plaintiffs in *Revitch* claimed that NaviStone acted  
 8 independently, including: “coordinat[ing] with additional entities,” “attempts to ‘match’ elements  
 9 of the intercepted data with records of real-life people [NaviStone] maintained in the back-end  
 10 databases,” “combining and correlating its data, [so that] NaviStone can watch consumers as they  
 11 browse hundreds of participating e-commerce sites, in real-time,” “obfuscat[ing] the wiretap codes  
 12 through dummy domains to attempt to conceal its activities,” and independently “send[ing]  
 13 postcards to the homes of anonymous website shoppers within a day or two of their visit,” matching  
 14 anonymous site traffic to names and addresses, among other things. *Id.* ¶¶ 18, 19, 21, 22. No such  
 15 facts are pled here. At most, Plaintiffs allege that some unspecified FullStory technology that may  
 16 or may not have been implemented by Noom and may have allowed FullStory to review and parse  
 17 data it collected as a service provider in the context of providing that service. These speculative  
 18 allegations are a far cry from those at issue in *Revitch* and *Facebook*. *See supra* section II.

19 Given that there is no equivalent of a wiretap here, FullStory is not a third-party  
 20 eavesdropper and Noom cannot be liable for aiding or conspiring with FullStory regarding the  
 21 alleged wiretap. Plaintiffs' Section 631 claims should be dismissed on these grounds as well.

22 **c. Even if FullStory's technology is a wiretap, Plaintiffs fail to plead  
 23 that the content of their communications was intercepted.**

24 Plaintiffs allege that the “actionable ‘content’ . . . falls under two categories” which include  
 25 “webpages and URLs that Plaintiffs viewed while on the website” and “Plaintiffs’ keystrokes,  
 26 mouse clicks, form field entries, and another information Plaintiffs intentionally provided to Noom  
 27 while on the website.” (SAC ¶ 89.) Despite this Court’s directive that Plaintiffs “delineate content  
 28 from non-content records,” Plaintiffs fail both to correctly define content and to sufficiently plead

1 what, if any, of their content was intercepted. (ECF No. 51 at 10.) **First**, neither “webpages and  
 2 URLs” nor “keystrokes” or “mouse clicks” are actionable content under CIPA. (SAC ¶ 89.) *See*  
 3 *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014) (reasoning that “divulge[ing]  
 4 identification and address information contained in a referer header,” as well as “record  
 5 information” are not the contents of a communications under the Wiretap Act).

6 **Second**, even after two opportunities to amend, Plaintiffs remain unable to identify what, if  
 7 any, specific information they input on Noom’s website, merely alleging that they “filled out  
 8 portions of the form on Noom’s website,” and that they input “at least some” unspecified “personal  
 9 and medical information.” (SAC ¶¶ 4, 5, 50, 51.) Plaintiffs likewise never allege what specific  
 10 “form field entries” or other information they entered when visiting Noom’s website. (*See, e.g., id.*  
 11 ¶ 89.) Plaintiffs thus fail to plausibly allege that they provided Noom any actionable content. *See*  
 12 Order Dismissing First Am. Compl. with Leave to Amend at 1, *Revitch v. New Moosejaw, LLC*,  
 13 No. 3:18-cv-06287 (N.D. Cal. May 1, 2019), ECF No. 40 (dismissing similar claims for lack for  
 14 Article III standing because “[w]ithout any allegations about the content of the communications  
 15 Revitch had with New Moosejaw or NaviStone, or about the files accessed from his computer,  
 16 Revitch has not identified a concrete and particularized harm.”).

17 As set forth above, this Court should dismiss with prejudice Plaintiffs’ Section 631 claims  
 18 for failing to sufficiently plead that FullStory intercepted the content of their communications.

19 **2. Plaintiffs Fail to Allege Sufficient Facts to Support a Section 635 Claim.**

20 Plaintiffs claim that by “enabling FullStory to wiretap visitors to its Website, Noom  
 21 possessed and used a wiretap device that is primarily or exclusively designed or intended for  
 22 eavesdropping upon the communication of another.” (SAC ¶ 101.) This claim should also be  
 23 dismissed with prejudice, regardless of whether Plaintiffs’ Section 631 claims are sustained.<sup>6</sup>

24  
 25 <sup>6</sup> If Plaintiffs’ Section 631 claims survive, their Section 635 claims may still be insufficient, and  
 26 vice versa. To read otherwise would “confuse[] ... alleged violations of § 2512 with violations of  
 27 § 2511.” *Allen v. Quicken Loans Inc.*, No. 17-12352, 2018 WL 5874088, at \*9 (D.N.J. Nov. 9,  
 28 2018) (citing *Luis v. Zang*, 833 F.3d 619, 644 (6th Cir. 2016) (Batchelder, J. dissenting)). Such an  
 interpretation would also render Section 635 redundant with Sections 631 and 632, given that, in  
 order to allegedly eavesdrop or wiretap (and thus violate Sections 631 or 632), one must possess  
 the alleged eavesdropping/wiretapping device (Section 635). This is in accord with the “cardinal  
 rule of statutory interpretation that no provision should be construed to be entirely redundant.”  
*Republic of Ecuador v. Mackay*, 742 F.3d 860, 864 (9th Cir. 2014) (citation omitted).

a. Plaintiffs lack constitutional or statutory standing to bring a Section 635 claim against Noom.

3 To start, Plaintiffs lack both constitutional and statutory standing to pursue a Section 635  
4 claim because CIPA’s private right of action cannot be extended to permit suits predicated on the  
5 mere “possession” of or enabling others to use an alleged eavesdropping device. As to statutory  
6 standing, CIPA only grants a private right of action to “[a]ny person who has been injured by a  
7 violation of this chapter . . . .” Cal. Penal Code § 637.2(a). Likewise, to satisfy Article III standing,  
8 a plaintiff must allege “injury in fact,” *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). To  
9 meet this standard, a plaintiff “must show that . . . she suffered an invasion of a legally protected  
10 interest that is concrete and particularized” from the alleged violation, and that the defendant’s  
11 actions “affect[ed] the plaintiff in a personal and individual way.” *Id.* at 1548 (citation omitted).

12       Here, Plaintiffs do not meet either standard because they only allege that Noom possessed  
13 a wiretap device and Plaintiffs still identify no accompanying cognizable injury as a result of this  
14 possession—presumably because they have suffered none.<sup>7</sup> This is unsurprising, as possession of  
15 a device is not connected to any injury, real or imagined, and so cannot meet the *Spokeo* standard.

16        In *Cohen*, for example, the court held that it would be “constitutionally problematic” to  
17    accord a private right of action for possession of a wiretap device such that “plaintiffs who suffered  
18    no injury in fact would still be able to sue.” *Cohen v. Casper Sleep, Inc.*, Nos. 17cv9325, 17cv9389,  
19    17cv9391, 2018 WL 3392877, at \*5 (S.D.N.Y. July 12, 2018) (citation omitted). The same  
20    reasoning holds here. *See NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 954 (N.D.  
21    Cal. 2014) (“The analysis for a violation of CIPA is the same as that under the federal Wiretap  
22    Act.”). Allowing suit for possession of an eavesdropping device, without any allegation of injury,  
23    would obviate the need for Article III standing and raise serious constitutional concerns.

24 The court in *Revitch* incorrectly reached a different conclusion, holding that plaintiffs had  
25 sufficiently pled injury by simply parroting the statutory requirements and “alleg[ing] injuries

<sup>7</sup> Plaintiffs state in passing that Noom somehow “used” a wiretap “by enabling FullStory to wiretap visitors to its Website” (SAC ¶ 101), but this allegation is not plausible. Enabling another to use a device is not the same as actually using the device—indeed, such an interpretation would be an unprecedented expansion of Section 635 liability.

1 traceable to Moosejaw’s possession and use of the device.” *Revitch*, 2019 WL 5485330, at \*3. The  
 2 court’s decision in *Revitch* is contrary to the plain language of the statute as well as the decisions  
 3 of many other courts that have made clear that CIPA’s federal analogue, the Wiretap Act, does not  
 4 provide a private right of action for the manufacture, possession, and/or sale of wiretap devices.  
 5 *See In re Lenovo Adware Litig.*, No. 15-md-02624, 2016 WL 6277245, at \*7 (N.D. Cal. Oct. 27,  
 6 2016) (“Section 2512 [federal Section 635 analogue] however, does not establish a private right of  
 7 action—it addresses only criminal liability.”); *see also DirecTV, Inc. v. Treworgy*, 373 F.3d 1124,  
 8 1129 (11th Cir. 2004) (concluding that “the language of section 2520(a) does not create a private  
 9 right of action against a person who possesses a device in violation of section 2512(1)(b)”).

10 Regardless, the facts as pled here are substantially different from those in *Revitch*. The  
 11 Plaintiffs in *Revitch* alleged that, among other things, NaviStone “scanned [plaintiff’s] computer  
 12 for files that revealed his identity and browsing habits.” *Revitch*, 2019 WL 5485330, at \*3. By  
 13 contrast, Plaintiffs here only contend that “FullStory—as enabled by Noom—captured, stored, and  
 14 analyzed Plaintiffs’ electronic communications,” (SAC ¶ 2); they had a “reasonable expectation  
 15 that their PII, PHI, and other data would remain confidential,” (*id.* ¶ 112); and that “session  
 16 recording technologies such as FullStory’s *can leave* users vulnerable to data leaks and the harm  
 17 resulting therefrom.” (*Id.* ¶ 34 (emphasis added).) Plaintiffs do *not* plead that Noom accessed their  
 18 information for an improper purpose; disclosed their information to any third party; or otherwise  
 19 caused them any harm whatsoever. *See supra* section II. These facts render *Revitch* inapposite and  
 20 are insufficient to demonstrate the required concrete injury. *Cf. Cahen v. Toyota Motor Corp.*, 717  
 21 F. App’x 720, 724 (9th Cir. 2017) (holding that claims of unauthorized data sharing of  
 22 non-individually identifiable driving history did not meet Article III standing requirements).

23 Accordingly, this Court should dismiss Plaintiffs’ Section 635 claim with prejudice.

24 **b. FullStory’s technology is not a device “primarily or exclusively  
 25 designed” for eavesdropping.**

26 Plaintiffs’ Section 635 claim fails for another reason as well. Aside from their bare recital  
 27 of the statute’s requirements, Plaintiffs fail to allege sufficient facts to show the alleged “code”  
 28 installed on Noom’s website is a device “primarily or exclusively designed” for eavesdropping. In

1 the absence of a statutory definition, courts “look to the plain meaning” of the disputed terms.  
 2 *Friends of Yosemite Valley v. Norton*, 348 F.3d 789, 796 (9th Cir. 2003). Merriam-Webster defines  
 3 eavesdropping as “the act of secretly listening to something private,” an allegation conspicuously  
 4 missing from Plaintiffs’ SAC. *Eavesdropping*, Merriam-Webster, <https://www.merriam-webster.com/dictionary/eavesdropping>; (SAC ¶¶ 100-102). As Plaintiffs note, the code simply  
 5 collects data willingly typed onto Noom’s website, much the same as “content from third-party  
 6 servers” is collected through “analytics tools, advertising networks, code libraries and other  
 7 utilities,” which are “part of routine internet functionality.” *In re Facebook Internet Tracking Litig.*,  
 8 263 F. Supp. 3d 836, 846 (N.D. Cal. 2017) (overturned on other grounds); *cf. Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (finding that LinkedIn did not commit a “highly  
 10 offensive” invasion of users’ privacy by disclosing users’ browsing histories to third parties); *In re Google, Inc. Priv. Pol’y Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (finding that Google’s  
 11 collection and disclosure of users’ data, including their browsing histories, “do not plausibly rise to  
 12 the level of intrusion necessary to establish an intrusion claim”).

13 While Plaintiffs assert that FullStory’s “code” is designed to collect non-confidential  
 14 keystroke information, they do not explain why that function makes it a device “primarily or  
 15 exclusively designed” for *eavesdropping*. (SAC ¶¶ 100-102.) Indeed, this code allegedly behaves  
 16 and is used in a manner identical to any technology designed to facilitate web-browsing activity,  
 17 including cookie technology, which can be used for a variety of purposes. *Cf., In re DoubleClick, Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001) (explaining how cookies are  
 18 computer programs commonly used by websites to store useful information that help with website  
 19 operation, just as session replay tools employ computer programs do as well).

20 Plaintiffs attempt to paint FullStory’s technology as more harmful than “run-of-the-mill”  
 21 website analytics such as “cookies” by alleging that cookies are not individualized. (SAC ¶ 33.)  
 22 Not so. As explained in *In re DoubleClick*, cookies are stored locally on website visitor machines  
 23 and can be used to create comprehensive, *individualized and identifiable*, profiles about website  
 24 visitors—something Plaintiffs do not allege Noom achieves with session replay technology. The  
 25 fact that FullStory may collect or present this data differently, as Plaintiffs allege, does not render

1 it more intrusive than what is collected by many cookies. (SAC ¶ 25, 49.)

2 Given Plaintiffs' failure to allege how this code was deployed to purportedly intercept her  
 3 electronic communications, or how this code is exclusively used for eavesdropping and therefore  
 4 could be considered a device within the meaning of the statute, Plaintiffs fail to state a claim under  
 5 Section 635 and this cause of action should be dismissed with prejudice.

6 **B. Plaintiffs Fail to Allege an Invasion of Privacy Under the California  
 7 Constitution.**

8 Plaintiffs also do not state a claim under the California Constitution for multiple reasons.  
 9 As this Court recognized in dismissing the First Amended Complaint, Plaintiffs' California  
 10 Constitution claims cannot survive because they fail to state a claim under CIPA. (ECF No. 51 at  
 11 13.) Moreover, regardless of whether the Court sustains Plaintiffs' CIPA claims, the invasion of  
 12 privacy claims must be dismissed because Plaintiffs' amended allegations do not meet the "high  
 13 bar for an invasion of privacy claim." *Belluomini v. Citigroup, Inc.*, No. CV 13-01743, 2013 WL  
 14 3855589, at \*6 (N.D. Cal. July 24, 2013); *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)  
 15 (describing the necessary violation for a California Constitutional invasion of privacy claim as one  
 16 "so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of  
 17 the social norms.") (internal quotation marks and citation omitted).

18 To plead a claim for invasion of privacy under the California Constitution, Plaintiffs must  
 19 allege: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the  
 20 circumstances; and (3) conduct by the defendant that amounts to a serious invasion of a protected  
 21 privacy interest." *Moreno v. S.F. Bay Area Rapid Transit Dist.*, No. 17-cv-02911, 2017 WL  
 22 6387764, at \*7 (N.D. Cal. Dec. 14, 2017).

23 Plaintiffs' SAC falls short of these standards because they do not allege how the browsing  
 24 conduct on Noom's website is "sensitive and confidential," nor do they explain how they had a  
 25 reasonable expectation of privacy *from Noom or its service providers* as to information they  
 26 voluntarily input on Noom's website. *See, e.g., In re Yahoo Mail Litig. (Yahoo)*, 7 F. Supp. 3d  
 27 1016, 1040 (N.D. Cal. 2014) (internal quotation and citation omitted) (finding that there is no legally  
 28 protected privacy interest in the contents of emails generally, only in content that is sensitive and

1 confidential). In fact, Plaintiffs' SAC still fails to allege facts establishing *any* of these elements,  
 2 much less all three, and therefore the Court should dismiss this claim with prejudice.

3 **1. Plaintiffs Fail to Allege a Legally Protected Privacy Interest.**

4 To withstand dismissal of an invasion of privacy claim, Plaintiffs must allege a legally  
 5 protected privacy interest. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35 (1994). "Just as  
 6 the right to privacy is not absolute, privacy interests do not encompass all conceivable assertions  
 7 of individual rights." *Id.* Legally recognized privacy interests are generally categorized in "two  
 8 classes: (1) interests in precluding the dissemination or misuse of *sensitive and confidential*  
 9 *information* ('informational privacy'); and (2) interests in making intimate personal decisions or  
 10 conducting personal activities without intrusion ('autonomy privacy')." *Id.* (emphasis added).

11 Plaintiffs parrot these legal requirements and generally allege that they have an interest in  
 12 "precluding the dissemination and/or misuse" of their information, and in making personal  
 13 decisions and/or conducting personal activities without observation. (SAC ¶ 110). Yet they fail to  
 14 plead facts to establish a legally protected informational privacy *or* autonomy privacy interest.

15 Autonomy privacy is akin to bodily autonomy (such as a right to obtain an abortion or to  
 16 not provide urine for a drug test) and courts have not found "cause to extend the bodily autonomy  
 17 line of cases to data autonomy." *In re Google Location Hist. Litig.*, 428 F. Supp. 3d 185, 198 (N.D.  
 18 Cal. 2019); *Yahoo*, 7 F. Supp. 3d at 1039 ("California courts have discussed autonomy privacy in  
 19 the context of cases alleging *bodily* autonomy."). The information potentially at issue here—*i.e.*,  
 20 age, gender, diet and weight loss information input on a public website that Plaintiffs do not even  
 21 allege is linked to their identity—has nowhere near the same privacy interest recognized in cases  
 22 involving bodily autonomy, and Plaintiffs have thus not pled a legally protected privacy interest on  
 23 this theory. *Contra Smith v. Fresno Irrigation Dist.*, 72 Cal. App. 4th 147, 161 (1999) (discussing  
 24 autonomy privacy in the context of drug testing through use of a urine sample).

25 Plaintiffs also fail to plead an informational privacy interest for multiple reasons. *First*,  
 26 most personally identifying information is not subject to constitutional protection. "The disclosure  
 27 of mere contact information, such as names and addresses, does not unduly interfere with one's  
 28 right to privacy." *Cabral v. Supple, LLC*, No. EDCV 12-85, 2012 WL 12895825, \*3 (C.D. Cal.

1 Oct. 3, 2012). Indeed, even in the context of private *medical* information, courts have held that  
 2 “[p]laintiff and the [c]lass have no legally protected privacy interest in de-identified  
 3 information.” *London v. New Albertson’s, Inc.*, No. 08-CV-1173, 2008 WL 4492642, at \*8 (S.D.  
 4 Cal. Sept. 30, 2008) (dismissing invasion of privacy claim). Similarly, Noom has not disavowed  
 5 promises regarding the treatment of the data website users provide it. *Contra In re Vizio, Inc.*,  
 6 *Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (finding that when courts  
 7 “extend the tort of invasion of privacy to the routine collection of personally identifiable  
 8 information” it involves surreptitious collection or “disregard[ing] consumers’ privacy choices”).  
 9 Plaintiffs do not allege what specific information they disclosed to Noom, and their conclusory  
 10 claim that such information was sensitive does not make it so. *See supra* section II.

11 *Second*, courts reject the application of information privacy claims where—as here—the  
 12 defendants “only tracked and collected data during use of [defendant’s] services.” *In re Google*  
 13 *Location Hist. Litig.*, 428 F. Supp. 3d at 198.

14 *Third*, Plaintiffs do not plead, as they must, that the information they provided to Noom was  
 15 “disseminat[ed]” or “misuse[d]” in any fashion. *Hill*, 7 Cal. 4th at 35; *see also Alch v. Superior*  
 16 *Ct.*, 165 Cal. App. 4th 1412, 1423 (2008) (“Informational privacy . . . is the interest ‘in precluding  
 17 the dissemination or misuse of sensitive and confidential information.’”) (citation omitted). While  
 18 Plaintiffs may claim that they have properly pled “dissemination” because the data collected on  
 19 Noom’s behalf was allegedly available to FullStory, nowhere do they allege that any data was  
 20 disseminated beyond Noom’s service provider or that FullStory did or could even potentially  
 21 misuse any information that was purportedly collected. Nor do they allege that the information  
 22 they provided was linked to their identities. Plaintiffs only allege the information was shared with  
 23 FullStory as Noom’s service provider to be used only for Noom’s purposes. (SAC ¶ 12, 13.) These  
 24 allegations plainly do not satisfy the “dissemination” or “misuse” requirement.

25 **2. Plaintiffs Fail to Allege a Reasonable Expectation of Privacy.**

26 Plaintiffs’ privacy claim also fails because they do not plead that they had a reasonable  
 27 expectation of privacy. “A ‘reasonable’ expectation of privacy is an objective entitlement founded  
 28 on broadly based and widely accepted community norms.” *Hill*, 7 Cal. 4th at 37 (citation omitted).

1 In determining whether an “objective entitlement” is present, “customs, practices, and [the]  
 2 physical settings surrounding particular activities” are taken into consideration, as are “*advance*  
 3 *notice*” and “the presence or absence of opportunities to *consent voluntarily* to activities impacting  
 4 privacy interests.” *Id.* at 36-37 (emphasis added). Further, “[t]he plaintiff in an invasion of privacy  
 5 action must have conducted himself or herself in a manner consistent with an actual expectation of  
 6 privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the  
 7 invasive actions of defendant.” *Yahoo*, 7 F. Supp. 3d at 1037-38 (internal citations omitted).

8 While Plaintiffs generically contend that they “had a reasonable expectation that their PII,  
 9 PHI, and other data would remain confidential,” Plaintiffs cannot credibly claim they expected that  
 10 their communications with Noom’s website should be hidden from **Noom**. (SAC ¶ 112, 48.) Far  
 11 from being hidden, their interactions with Noom’s website were themselves intentional  
 12 communications with Noom’s servers. *See Cohen*, 2018 WL 3392877, at \*3 (analyzing similar  
 13 claims and finding “[i]t is clear that the Retailers were parties to the communications . . .”).<sup>8</sup>

14 Noom anticipates that Plaintiffs will argue that their communications should have been kept  
 15 confidential from Noom’s own service providers. Yet Plaintiffs fail to allege any facts creating an  
 16 inference that such an expectation was **reasonable**. Plaintiffs have not alleged, for example, that  
 17 Noom expressly informed users that their communications would remain private. Nor could they:  
 18 Noom explicitly discloses to Plaintiffs in its privacy policy that data regarding their interactions  
 19 with the website may be collected by Noom **and by Noom’s service providers**.<sup>9</sup>

20 Moreover, virtually all consumer-facing websites track the conduct of web visitors for  
 21 myriad reasons, including enhancing the browsing experience and site functionality. This tracking  
 22 is accomplished by a similar myriad of third-party service providers. Any web user who has  
 23 enabled Ghostery or similar browser plug-ins to track the third party tools used by the websites  
 24

25 <sup>8</sup> The online articles Plaintiffs reference are not to the contrary—they in fact confirm that when  
 26 users visit a website “[t]his data can’t reasonably be expected to be kept anonymous” from that first  
 27 party website. (SAC ¶ 69 (citing Steven Englehardt, *No boundaries: Exfiltration of personal data*  
 28 *by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>)).

<sup>9</sup> See *Privacy Policy*, Noom (Dec. 17, 2018), <https://web.noom.com/terms-and-conditions-of-use/noom-privacy-policy>.

1 they visit can attest that this is true.<sup>10</sup> Given the near-universal practice of consumer-facing  
 2 websites, no user can reasonably expect that the web pages she visits, or the information she  
 3 provides to the operator of such a website, are hidden from that operator or its service providers.

4 **3. Plaintiffs Fail to Allege Noom’s Conduct Was a Serious Invasion of  
 5 Privacy.**

6 Even if Plaintiffs had a legally protectable and objectively reasonable expectation that no  
 7 party could view their activity on Noom’s website, Noom’s alleged monitoring would still not be  
 8 highly offensive or meet the “high bar” for a common law invasion of privacy claim. *See Low*, 900  
 9 F. Supp. 2d at 1025 (noting the high bar for such claims). To be a serious invasion of privacy  
 10 requires the alleged conduct to be an egregious violation of social norms. *Yahoo*, 7 F. Supp. 3d at  
 11 1042. Notably, courts have held that even the collection and subsequent dissemination of user data  
 12 for marketing purposes is not a serious invasion of privacy. *See In re Google Inc. Priv. Pol’y Litig.*,  
 13 58 F. Supp. 3d at 987-88 (rejecting an invasion of privacy claim for collecting location information  
 14 from users, associating it with other private user information, and then disclosing the commingled  
 15 data to “third-party developers” in ways that allegedly violate the defendant’s own policies). It  
 16 cannot be, then, that the routine analysis of web activity for purposes of analyzing website design  
 17 and customer experience passes this high bar.

18 The California Court of Appeals’ decision in *Folgelstrom v. Lamps Plus, Inc.* is instructive.  
 19 There, plaintiff asserted claims based on the collection of personally identifiable information that  
 20 was shared with third-party marketing firms. 195 Cal. App. 4th 986, 992 (2011). The court found  
 21 “obtaining plaintiff’s [information] without his knowledge or permission, and using it [for marketing  
 22 purposes] . . . is not an egregious breach of social norms, but routine commercial behavior.” *Id.*  
 23 The equally routine and much less invasive practice of a website using its own customer  
 24 information to enhance its functionality—and employing third-party companies to act as a proxy in  
 25 said efforts—cannot therefore be an egregious violation of social norms that is highly offensive.  
 26 Indeed, Noom’s use of a third party to collect this information in an anonymized or pseudonymized  
 27

28 

---

<sup>10</sup> Ghostery and similar tools enable their users to detect and control tags, trackers, and beacons—including session replay scripts—embedded in web pages. *See* <https://www.ghostery.com/>.

1 manner is arguably *more* privacy protective, as it limits the ability of Noom or its third-party vendor  
 2 to deanonymize or create individual profiles from this data directly.

3 The court’s reasoning in *Folgelstrom* is consistent with a large body of case law in this  
 4 district that finds even the allegedly surreptitious collection and dissemination of personally  
 5 identifiably information, such as unique device identifiers, browsing activity, and address  
 6 information, for commercial purposes, is not enough to meet the exacting “highly offensive”  
 7 standard. *See, e.g., In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012)  
 8 (dismissing with allegations that defendants disclosed to third parties “the unique device identifier  
 9 number, personal data, and geolocation information from Plaintiffs’ iDevices”); *Yunker v. Pandora*  
 10 *Media, Inc.*, No. 11-CV-03113, 2013 WL 1282980, at \*14-15 (N.D. Cal. Mar. 26, 2013) (same  
 11 with allegations of “obtain[ing] [plaintiff’s] PII and provided that information to advertising  
 12 libraries for marketing purposes, in violation of the terms of Pandora’s Privacy Policy”); *In re*  
 13 *Google Android Consumer Priv. Litig.*, No. 11-MD-02264, 2013 WL 1283236, at \*2, \*9-11 (N.D.  
 14 Cal. Mar. 26, 2013) (same with allegations of tracking and sharing of “highly detailed and  
 15 confidential [PII] over a substantial period of time without [Plaintiffs’] knowledge or consent”).  
 16 Indeed, even negligent conduct that leads to theft of highly personal information, such as social  
 17 security numbers, does not “approach [the] standard” of actionable conduct under the California  
 18 Constitution and thus does not constitute a violation of Plaintiffs’ right to privacy. *See Ruiz v. Gap,*  
 19 *Inc.*, 540 F. Supp. 2d 1121, 1127-28 (N.D. Cal. 2008), *aff’d*, 380 F. App’x 689 (9th Cir. 2010).

20 Plaintiffs may point to two cases, *Facebook* and *Revitch*, to avoid dismissal, but neither is  
 21 availing. In *Facebook*, the court held that plaintiffs plausibly alleged an invasion of privacy based  
 22 on allegations that defendant created a comprehensive “cradle-to-grave profile” that “constantly  
 23 compiled and updated its database with the users’ browsing activities” on third party websites for  
 24 logged-out Facebook users. *Facebook*, 956 F.3d at 599. According to that court, plaintiffs  
 25 identified sufficient facts to survive a motion to dismiss based on “surreptitious data collection  
 26 when individuals were not using Facebook” and their allegations that “internal Facebook  
 27 communications reveal that the company’s own officials recognized these practices as a  
 28 problematic privacy issue.” *Id.* at 606 (emphasis added). No such allegations are pled here, and

1 any effort to contort that case to fit the facts alleged in the SAC—i.e., electronic communications  
 2 directly between a website user and its own visitors whose collection and analysis is facilitated by  
 3 a service provider—would be contrary to well-settled authority cited above.

4 Meanwhile in *Revitch*, the court relied on allegations that the code in question “scanned  
 5 [plaintiff’s] computer for files that revealed his identity and browsing habits.” *Revitch*, 2019 WL  
 6 5485330, at \*3. Those facts are not pled in this case. As explained above, the routine collection  
 7 of information provided to a first party website and its vendor cannot possibly satisfy the strict  
 8 standard for invasion of privacy claims under the California Constitution. Accordingly, neither  
 9 *Facebook* nor *Revitch* saves Plaintiffs’ invasion of privacy claims, and they too must be dismissed.

10 **V. PLAINTIFF MOISE’S CLAIMS FOR INJUNCTIVE RELIEF SHOULD BE DISMISSED PURSUANT  
 11 TO RULE 12(B)(1) BECAUSE SHE LACKS STANDING.**

12 Even if the Court finds that Plaintiffs state a claim under CIPA or the California  
 13 Constitution, it should nevertheless dismiss Plaintiff Moise’s claims for injunctive relief because  
 14 she again fails to plausibly allege a likelihood of future or continuing harm, as required for standing  
 15 to bring such a claim. *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983). Specifically, Plaintiff  
 16 Moise contends that she “would be willing to use Noom’s program,” subject to certain conditions.  
 17 (SAC ¶ 96.) Nowhere does she contend, as required, that she intends to use Noom in the future.  
 18 *See Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956, 971 (9th Cir. 2018) (recognizing that when  
 19 “standing for prospective injunctive relief is premised entirely on the threat of repeated injury” a  
 20 party must demonstrate “a sufficient likelihood that [s]he will again be wronged in a similar way.”)  
 21 (quoting *Lyons*, 461 U.S. at 111.) For this reason, Plaintiff Moise’s injunctive relief claims  
 22 necessarily fail and should be dismissed with prejudice.

23 **VI. CONCLUSION.**

24 For the reasons above, this Court should grant the Motion and dismiss the case against  
 25 Noom in its entirety, with prejudice. *See Eminence Cap., LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1052  
 26 (9th Cir. 2003).

27  
 28

1 Dated: May 27, 2021

COOLEY LLP

2 By: /s/ Michael Rhodes

3 Michael G. Rhodes

4 Attorneys for Defendant  
5 Noom, Inc.

250136075

6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28